CLAIMS

1. A method for securely removing a device from at least one of a plurality of devices in a network, the method comprising:

calculating an encryption key for a protected content in the network, based at least in part on a list of the plurality of devices in the network;

marking the device for removal, by modifying the list of the plurality of devices in the network;

recalculating the encryption key using the modified list; and

reencrypting the protected content with the recalculated encryption key.

2. The method of claim 1, further comprising the device to be removed acknowledging its removal.

3. The method of claim 2, further comprising denoting the acknowledgement in the modified list.

4. The method of claim 1, wherein recalculating the encryption key comprises including a key management block in the calculation.

5. The method of claim 1, wherein recalculating the encryption key comprises including an authorization table in the calculation.

6. The method of claim 1, wherein recalculating the encryption key comprises including the binding identification for the plurality of devices, excluding the device to be removed.

7. The method of claim 1, wherein the protected content is encrypted with a title key; and

further comprising reencrypting the title key with the recalculated encryption key.

8. A system for securely removing a device from at least one of a plurality of devices in a network, the system comprising:

an encryption key that is calculated for a protected content in the network, based at least in part on a list of the plurality of devices in the network;

the device being marked for removal by modifying the list of the plurality of devices in the network;

the encryption key being recalculated using the modified list; and

the protected content being reencrypted with the recalculated encryption key.

9. The system of claim 8, wherein the device to be removed acknowledges its removal.

10. The system of claim 9, wherein the acknowledgement of removal is reflected in the modified list.

11. The system of claim 8, wherein the encryption key is recalculated using a key management block in the calculation.

12. The system of claim 8, wherein the encryption key is recalculated using an authorization table in the calculation.

13. The system of claim 8, wherein the encryption key is recalculated using the binding identification for the plurality of devices, excluding the device to be removed.

14. The system of claim 8, wherein the protected content is encrypted with a title key; and

further comprising the title key being reencrypted with the recalculated encryption key.

15. The system of claim 8, wherein the plurality of devices comprise any one or more of:

a television, a set top box, a personal video recorder, a video cassette recorder, a compact disk player, a compact disk player recorder, a personal computer, a portable music player, an audio player, a video player, a game console, and a personal network storage device.

16. A method for securely removing a protected content from at least one of a plurality of devices in a network, the method comprising:

calculating an encryption key for the protected content in the network, based at least in part on a list of the previously removed content;

marking the protected content for removal, by modifying the list of the removed content;

recalculating the encryption key using the modified list; and

reencrypting the protected content with the recalculated encryption key.

17. The method of claim 16, further comprising removing a device from the plurality of devices from the network.

18. The method of claim 17, wherein the removed device acknowledges its removal; and

further comprising reflecting the acknowledgement of the removal in the modified list.

19. The method of claim 16, wherein recalculating the encryption key comprises including a key management block in the calculation.

20. The method of claim 16, wherein recalculating the encryption key comprises including an authorization table in the calculation.

21. The method of claim 16, wherein recalculating the encryption key comprises including the binding identification for the plurality of devices.

22. The method of claim 16, wherein the protected content is encrypted with a title key; and

further comprising reencrypting the title key with the recalculated encryption key.

23. A system for securely removing a protected content from at least one of a plurality of devices in a network, the system comprising:

an encryption key that is calculated for the protected content in the network, based at least in part on a list of the previously removed content;

the protected content to be removed being marked for removal by modifying the list of removed content;

the encryption key being recalculated using the modified list; and

the protected content being reencrypted with the recalculated encryption key.

24. The system of claim 23, wherein a device from the plurality of devices is removed from the network.

25. The system of claim 24, wherein the removed device acknowledges its removal; and

wherein the acknowledgement of the removal is reflected in the modified list.

26. The system of claim 23, wherein the encryption key is recalculated using a key management block in the calculation.

27. The system of claim 23, wherein the encryption key is recalculated using an authorization table in the calculation.

28. The system of claim 23, wherein the encryption key is recalculated using the binding identification for the plurality of devices.

29. The system of claim 23, wherein the protected content is encrypted with a title key; and

further comprising the title key being reencrypted with the recalculated encryption key.

30. The system of claim 23, wherein the plurality of devices comprise any one or more of:

a television, a set top box, a personal video recorder, a video cassette recorder, a compact disk player, a compact disk player recorder, a personal computer, a portable music player, an audio player, a video player, a game console, and a personal network storage device.

31. A method for recovering from a failure of a device from a plurality of devices in a network, the method comprising:

an operating device acquiring a secret network ID for the network based upon a secret relationship between an identity and a secret binding ID of the device;

calculating an encryption key for a protected content in the network based at least in part on the secret network ID; and

upon device failure, communicating with a service server with a priori knowledge of the secret relationship, and acquiring the secret network ID.

32. The method of claim 31, wherein calculating the encryption key comprises including a key management block in the calculation.

33. The method of claim 31, wherein calculating the encryption key comprises including an authorization table in the calculation.

34. The method of claim 31, wherein calculating the encryption key comprises including the binding identification for the plurality of devices, excluding the device that has failed.

35. The method of claim 31, wherein the secret relationship comprises an encryption of the secret network ID of the operating device with a secret key.

36. A system for recovering from a failure of a device from a plurality of devices in a network, the system comprising:

an operating device that acquires a secret network ID for the network based upon a secret relationship between an identity and a secret binding ID of the device;

an encryption key that is calculated for a protected content in the network based at least in part on the secret network ID; and

upon device failure, the system communicates with a service server with a priori knowledge of the secret relationship, and acquires the secret network ID.

37. The system of claim 36, wherein the encryption key is recalculated using a key management block in the calculation.

38. The system of claim 36, wherein the encryption key is recalculated using an authorization table in the calculation.

39. The system of claim 36, wherein the encryption key is recalculated using binding identifications for the plurality of devices, excluding the device that has failed.

40. The system of claim 36, wherein the secret relationship comprises an encryption of the secret network ID of the operating device with a secret key.

41. The method of claim 36, wherein the secret relationship is stored in a database maintained by the service server.

42. A method for allowing a content provider service to learn a secret binding ID in a network of a plurality of devices, the method comprising:

the content provider service joining the network as one of the plurality of devices;

the content provider identifying itself as a compliant external service provider;

excluding the joining content provider service from being counted against a maximum number of allowable devices in the network; and

providing an integrity check mechanism to confirm that the joining content provider service is network compliant.

43. The method of claim 42, wherein the integrity check mechanism comprises a message authentication code that is based on a key management block.

44. A system for allowing a content provider service to learn a secret binding ID in a network of a plurality of devices, the system comprising:

the content provider service joining the network as one of the plurality of devices;

the content provider identifying itself as a compliant external service provider;

the joining content provider service is not counted against a maximum number of allowable devices in the network; and

an integrity check mechanism that confirms that the joining content provider service is network compliant.

45. The system of claim 44, wherein the integrity check mechanism comprises a message authentication code that is based on a key management block.

46. A method for maintaining an integrity of a network containing a plurality of devices, the method comprising:

calculating an integrity check value for network files and network values;

comparing the calculated integrity check value to a saved integrity check value, to determine if any one of the network files and the network values has changed;

calculating an encryption key on the network files and network values; and

decrypting a protected content in the network using the encryption key.

47. The method of claim 46, wherein the network files comprise a file that contains a list of removed files.

48. The method of claim 47, wherein the network files further comprise a file that contains a list of deleted content.

49. The method of claim 48, wherein the files that contain the lists of removed files and deleted content are stored in at least two different datastores.

50. The method of claim 49, wherein the files that contain the lists of removed files and deleted content are contained in an authorization table.

51. The method of claim 50, wherein the network files contain a key management block.

52. The method of claim 50, wherein the network values contain a device binding ID.

53. The method of claim 46, wherein the integrity check value contains the encryption key.

54. The method of claim 46, further comprising restricting playback of a protected content in the network.

55. The method of claim 54, wherein restricting the playback of the protected content in the network comprises determining if the protected content has an associated geographic restriction.

56. The method of claim 55, wherein restricting the playback of the protected content in the network further comprises determining if a device to play the protected content has an associated geographic limitation.

57. The method of claim 56, wherein restricting the playback of the protected content in the network further comprises preventing the playback of the protected content if the geographic restriction of the protected content is not met.

58. The method of claim 56, wherein restricting the playback of the protected content in the network further comprises preventing the playback of the protected content if the geographic limitation of the device to play the protected content is not met.

59. The method of claim 56, further comprising determining a geographic location of the device to play the protected content.

60. The method of claim 59, wherein determining the geographic location of the device to play the protected content comprises determining the geographic location based on a connection of the device to a cable service.

61. The method of claim 59, wherein determining the geographic location of the device to play the protected content comprises determining the geographic location based on an internal GPS receiver.

62. The method of claim 59, wherein determining the geographic location of the device to play the protected content comprises querying a user about the device geographic location.

63. The method of claim 59, further comprising placing a limitation on the number of times the geographic location of the device may be changed.

64. A system for maintaining an integrity of a network containing a plurality of devices, the system comprising:

an integrity check value that is calculated for network files and network values;

the calculated integrity check value being compared to a saved integrity check value, to determine if any one of the network files and the network values has changed;

an encryption key that is calculated on the network files and network values; and

a protected content being decrypted in the network using the encryption key.

65. The system of claim 64, wherein the network files comprise a file that contains a list of removed files.

66. The system of claim 65, wherein the network files further comprise a file that contains a list of deleted content.

67. The system of claim 66, wherein the files that contain the lists of removed files and deleted content are stored in at least two different datastores.

68. The system of claim 67, wherein the files that contain the lists of removed files and deleted content are contained in an authorization table.

69. The system of claim 68, wherein the network files contain a key management block.

70. The system of claim 68, wherein the network values contain a device binding ID.

71. The system of claim 64, wherein the integrity check value contains the encryption key.

72. The system of claim 64, further comprising a playback restriction mechanism to restrict playback of a protected content in the network.

73. The system of claim 72, wherein the playback restriction mechanism determines if the protected content has an associated geographic restriction.

74. The system of claim 72, wherein the playback restriction mechanism determines if a device to play the protected content has an associated geographic limitation.

75. The system of claim 74, wherein the playback restriction mechanism prevents the playback of the protected content if the geographic restriction of the protected content is not met.

76. The system of claim 75, wherein the playback restriction mechanism prevents the playback of the protected content if the geographic limitation of the device to play the protected content is not met.

77. The system of claim 75, wherein the playback restriction mechanism further determines a geographic location of the device to play the protected content.

78. The system of claim 77, wherein the playback restriction mechanism determines the geographic location of the device based on a connection of the device to a cable service.

79. The system of claim 77, wherein the playback restriction mechanism determines the geographic location based on an internal GPS receiver.

80. The system of claim 77, wherein the playback restriction mechanism queries a user about the device geographic location.

81. The system of claim 77, wherein the playback restriction mechanism places a limitation on the number of times the geographic location of the device may be changed.

82. A method for updating an existing key management block in a network of a plurality of devices, the method comprising:

determining if a current key management block is more recent than the existing key management block; and

if the current key management block is more recent than the existing key management block, the plurality of devices in the network accepting the current key management block.

83. The method of claim 82, wherein determining if the current key management block is more recent than the existing key management block comprises placing a revision number in the current key management block.

84. The method of claim 83, wherein the revision number is represented by a revision date.

85. The method of claim 83, further comprising signing the current key management block.

86. The method of claim 85, wherein determining if the current key management block is more recent than the existing key management block comprises the plurality of devices in the network verifying a signature of the current key management block.

87. The method of claim 86, further comprising the plurality of devices in the network accepting the current key management block network if, and only if the signature is verified.

88. The method of claim 86, further comprising the plurality of devices in the network accepting the current key management block network if, and only if the revision number in the current key management block is not older than a revision number in the existing key management block.

89 The method of claim 82, wherein determining if the current key management block is more recent than the existing key management block comprises comparing the revocation lists in the two key management blocks.

90. A system for updating an existing key management block in a network of a plurality of devices, the system comprising:

a current key management block that is compared for recency relative to the existing key management block; and

if the current key management block is more recent than the existing key management block, the plurality of devices in the network accept the current key management block.

91. The system of claim 90, wherein if the current key management block is more recent than the existing key management block, a revision number is placed in the current key management block.

92. The system of claim 91, wherein the revision number is represented by a revision date.

93. The system of claim 91, wherein the current key management block is signed.

94. The system of claim 93, wherein if the current key management block is more recent than the existing key management block, the plurality of devices in the network verify a signature of the current key management block.

95. The system of claim 94, wherein the plurality of devices in the network accept the current key management block network if, and only if the signature is verified.

96. The system of claim 94, wherein the plurality of devices in the network accept the current key management block network if, and only if the revision number in the current key management block is not older than a revision number in the existing key management block.

97 The system of claim 90, wherein the plurality of devices in the network accept the current key management block if the list of revoked devices in the current key management block is not less than the list of revoked devices in the existing key management block.